

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF DELAWARE

FORTINET, INC.,

Plaintiff,

v.

FIREEYE, INC.,

Defendant.

C. A. No. 12-1066 (SLR)

**JURY TRIAL DEMANDED**

**FIRST AMENDED COMPLAINT**

Plaintiff Fortinet, Inc. (“Fortinet”) for its First Amended Complaint against Defendant FireEye, Inc. (“FireEye”) alleges upon knowledge as to itself and its own actions and upon information and belief as to all other matters as follows:

**INTRODUCTION**

1. Fortinet brings this action against FireEye to seek remedies for FireEye’s infringement of U.S. Patent Nos. 8,056,135 (“the ‘135 Patent”), 8,204,933 (“the ‘933 Patent”), 7,580,974 (“the ‘974 patent”), 7,979,543 (“the ‘543 patent”), 8,051,483 (“the ‘483 patent”), and 8,276,205 (“the ‘205 patent”) (collectively, the “Asserted Patents”).

2. Fortinet also brings this action against FireEye to seek remedies for FireEye’s (i) deliberate and willful misappropriation of Fortinet trade secrets, (ii) intentional interference with one or more Fortinet contracts, and (iii) intentional interference with one or more prospective Fortinet economic advantages or relations, all of which caused and continue to cause significant harm to Fortinet.

**PARTIES**

3. Fortinet is a Delaware corporation with a principal place of business at 1090 Kifer Road, Sunnyvale, California 94086. Since 2000, Fortinet has been a leading provider of network security appliances, appliances and services, and a market leader in Unified Threat

Management systems. Fortinet currently employs 1800 individuals worldwide to serve its more than 125,000 customers around the globe.

4. On information and belief, FireEye is a corporation organized under the laws of Delaware with a principal place of business at 1440 McCarthy Blvd., Milpitas, California 95035.

### **JURISDICTION AND VENUE**

5. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a) because this lawsuit is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 101 *et seq.* This Court has supplemental jurisdiction over Fortinet's related state law claims pursuant to 28 U.S.C. § 1367.

6. This Court has personal jurisdiction over FireEye. On information and belief, FireEye has significant contacts with this forum and conducts and has conducted business within this forum and within this District. On information and belief, FireEye makes infringing products that are and have been offered for sale, sold, purchased, and used in this District. On information and belief, FireEye directly and/or through its sales and distribution network—including partners, subsidiaries, distributors, retailers, third party administrators, and/or others—places infringing products within the stream of commerce with the knowledge and/or understanding that such infringing products will be sold and used in this District. On information and belief, FireEye is a Delaware corporate entity, and also has a registered agent in this District for the purposes of accepting service of process. FireEye thus lacks any objection to this Court's personal jurisdiction.

7. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because FireEye resides in this District and because a substantial part of the events or

omissions giving rise to these claims occurred in this District including FireEye's acts of patent infringement.

### **FACTUAL BACKGROUND**

8. Founded in 2000, Fortinet is a leader and worldwide provider of innovative network security appliances and unified threat management solutions. In just over a decade, Fortinet has earned the trust of thousands of companies that use Fortinet's market-leading security solutions to protect their critical networks, databases, and applications. Fortinet's worldwide customers represent all verticals, including leading telecommunication carriers and multi-national enterprises.

9. Fortinet is a pioneer in the fields of network security and unified threat management and has expended substantial resources researching and developing its technology. This research and development has led to numerous innovative products in the network security market. The United States Patent and Trademark Office has recognized Fortinet's achievements by awarding numerous patents to Fortinet and its inventors as a result of these innovations. In addition to these Fortinet patents, Fortinet also owns other patents in the network security field that it has acquired over the past decade.

10. On information and belief, since around 2004, Fortinet has competed with FireEye in the network security industry.

### **FireEye's Corporate Raiding of Fortinet**

11. Since entering the network security market, FireEye has sought to acquire business and engineering expertise in the industry. But instead of relying on its own ingenuity and lawful business practices, FireEye's growth strategy has included competitor raids and trade secret misappropriation.

12. Since 2008, FireEye has hired at least eleven Fortinet employees from Fortinet's key divisions, including Fortinet product managers, marketing experts, security and systems engineers, account managers, and senior sales managers (hereinafter, the "Former Fortinet Employees"). Nine of these Former Fortinet Employees—including Fortinet's former Vice President of Product Management and Product Marketing—were hired in the past two and a half years.

#### **Fortinet's Trade Secrets**

13. Throughout the Former Fortinet Employees' employment at Fortinet, they received, acquired intimate knowledge of, and were otherwise privy to highly sensitive and valuable trade secret information about Fortinet customers (lists, contacts, sales data, trends, preferences, financials, leads), partners (lists, contacts, financials, distribution channels), Fortinet products (business plans, marketing, sales, pricing, tests, competitive intelligence), unique Fortinet employment information (proprietary compilations of data with salary and compensation package information), among other information (collectively, the "Fortinet Trade Secrets"). And when they left for FireEye, the Former Fortinet Employees illegally took these valuable Fortinet Trade Secrets with them for the benefit of FireEye.

14. At all relevant times, Fortinet took reasonable and necessary precautions to guard the secrecy and safety of the Fortinet Trade Secrets. Fortinet protects its facilities, servers, computers, networks, databases, and communications systems using a variety of physical and electronic security systems, such as access cards, password protection systems, firewalls, and encrypted communications technology. Fortinet also requires its employees—including the Former Fortinet Employees—to read, acknowledge, and sign an employment

agreement and/or a proprietary information and inventions agreement swearing them to secrecy and loyalty.

15. The employment agreement explicitly informs all employees that Fortinet's "proprietary information is extremely important" and that employment is "expressly subject to your executing a Proprietary Information and Inventions Agreement." The Former Fortinet Employees thus executed a Proprietary Information and Inventions Agreement and agreed that: "At all times during the term of my employment and thereafter, I will hold in strictest confidence and will not disclose, use, lecture upon or publish any of the Company's Proprietary Information," which includes, among other information, "information regarding plans for research, development, new products, marketing and selling, business plans, budgets and unpublished financial statements, licenses, prices and costs, suppliers and customers; and information regarding the skills and compensation of other employees of the Company."

16. The Former Fortinet Employees also agreed "that for the period of my employment by the Company and for one (1) year after the date of termination of my employment by the Company, I will not (i) induce any employee of the Company to leave the employ of the Company or (ii) solicit business of any client or customer of the Company (other than on behalf of the Company)."

17. On information and belief, prior to hiring the Former Fortinet Employees, FireEye knew or had reason to know of the Former Fortinet Employees' contractual obligations regarding confidential and valuable Fortinet Trade Secrets; FireEye decided to and did interfere with those contracts by causing or substantially causing their breach.

**FireEye's Theft of Fortinet Trade Secrets**

18. Despite their contractual obligations to Fortinet, the Former Fortinet Employees worked with FireEye, a Fortinet competitor, while employed by Fortinet and after employed by Fortinet, and failed to disclose that work to Fortinet. While the Former Fortinet Employees were employed by Fortinet and thereafter, the Former Fortinet Employees misappropriated and misused Fortinet property and Fortinet resources for the benefit of themselves and FireEye, and thereby breached their contractual obligations with Fortinet and violated state law trade secret protections.

19. On information and belief, FireEye willfully engaged in a systematic hiring spree of Fortinet employees in order to illegally acquire and improperly enrich itself from the Fortinet Trade Secrets. FireEye since has used and benefited from the Fortinet Trade Secrets without permission from or compensation to Fortinet.

**The Law Firm Account**

20. For example, one Former Fortinet Employee ("Employee 1") signed his engagement letter with FireEye on a Monday in August 2012, unbeknownst to Fortinet. Two days later, on Wednesday, and while still employed at Fortinet, Employee 1 received internal confidential Fortinet emails regarding a significant account with a large international law firm ("Law Firm"). As is common, the Law Firm was comparing two security providers, Fortinet and FireEye. Employee 1—just days after signing the FireEye engagement letter—was copied on and was actively engaged in preparing a detailed comparison of Fortinet's and FireEye's offerings in response. That same day, Employee 1 surreptitiously forwarded relevant emails related to the Law Firm account and containing and reflecting Fortinet Trade Secrets from his Fortinet email account to his personal email account. On information and belief, Employee 1

stole these Fortinet Trade Secrets in order to compete with Fortinet for at least the Law Firm account, among potentially other sales to Fortinet customers.

21. On information and belief, neither Employee 1 nor FireEye disclosed any of this information to Fortinet.

22. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Employee 1 by these improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets stolen by Employee 1 without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of themselves and others. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

23. FireEye also knowingly and intentionally induced, or attempted to induce, at least Employee 1 to violate his or her contractual obligations to Fortinet by stealing Fortinet Trade Secrets related to at least the Law Firm account.

24. Further, FireEye and Employee 1 deliberately intended to disrupt the business relationship between Fortinet and the Law Firm by stealing Fortinet Trade Secrets by and through forwarding Fortinet emails to a personal email account immediately before leaving Fortinet for FireEye. FireEye and Employee 1 were aware of Fortinet's relationship and/or potential relationship with the Law Firm yet stole Fortinet Trade Secrets related to the Law Firm for the use of FireEye, and thus willfully and intentionally interfered with that potential economic advantage to Fortinet's detriment.



### **International Distributor**

25. Fortinet has a significant relationship with a large, international distributor and reseller of network security appliances (the “Distributor”). On information and belief, a Former Fortinet Employee (“Employee 2”) was, while employed at Fortinet, a primary Fortinet contact and liaison with the Distributor for sales to Mexico and Latin America.

26. Distributors and resellers like the Distributor are critical to Fortinet’s sales channel, as they provide Fortinet with access to new markets, territories, and customer bases and typically provide high quality service and support. Trusted and well-respected distributors and resellers are valuable to companies like Fortinet and FireEye.

27. Fortinet’s internal list of distributors and resellers—and the history and terms of those relationships—are protected, confidential, and extremely valuable to Fortinet.

28. Employee 2’s last day at Fortinet was a Friday in August 2012. But shortly thereafter—that same month—Employee 2 began contacting and soliciting the Distributor on behalf of FireEye using Fortinet Trade Secrets. Employee 2 unlawfully attempted both to forge a new relationship with the Distributor for FireEye based on Fortinet Trade Secrets and to disrupt Fortinet’s relationship with the Distributor.

29. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Employee 2 by improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets without Fortinet’s consent and without regard to Fortinet’s rights, and without compensation, permission, or licenses for the benefit of themselves and others. FireEye’s conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet’s valid and enforceable rights.



30. FireEye also knowingly and intentionally induced, or attempted to induce, at least Employee 2 to violate his or her contractual obligations to Fortinet by stealing Fortinet Trade Secrets related to the Distributor.

31. Further, FireEye and Employee 2 deliberately intended to disrupt the business relationship between Fortinet and the Distributor by stealing Fortinet Trade Secrets in the form of distributor lists and the terms of history of Fortinet's relationship with the Distributor. FireEye and Employee 2 were aware of Fortinet's relationship and/or potential relationship with the Distributor yet stole Fortinet Trade Secrets related to the Distributor for use against Fortinet, and thus willfully and intentionally interfered with that potential economic advantage to Fortinet's detriment.

#### **Fortinet's Salesforce Database**

32. Fortinet maintains many Fortinet Trade Secrets on a confidential and secure data repository hosted by Salesforce.com ("Salesforce Database"). The Salesforce Database contains unique, proprietary Fortinet information considered to be the "crown jewels" of Fortinet's sales team. The Salesforce Database maintains information such as (i) lists of all the Fortinet customer accounts; (ii) billing addresses, shipping addresses, contact information, emails, telephone numbers, contracts, and contact history; (iii) specific customer, distributor, and partner contact information including titles, telephone numbers, email addresses, "if primary" contact, and other certification information; (iv) an "opportunities" page with details about what various account(s) are looking to buy, product lists, sales stage history, and leads (new, current, or future customers); (v) "special pricing requests" which shows Fortinet products and how much of a discount may have been given, who the distributor was, and how much margin the

distributor made, among other information; and (vi) forecasts, dashboards, and reports, through which Fortinet sales representatives or managers are able to view forecasts and run sales reports.

33. To access the Salesforce Database, a Fortinet employee first must be pre-approved and granted access by a Fortinet system administrator—at least one such administrator is one of the Fortinet employees raided by FireEye in 2012. This includes having a personal account created with a unique user name and private password. Accounts to Fortinet's Salesforce Database are limited and controlled by Fortinet—only employees who have a “need to know” are given access due to the highly sensitive, valuable Fortinet information contained in the database.

34. Knowing that much of Fortinet's most sensitive, valuable sales information resided in the Salesforce Database, in the days and weeks leading up to their departure from Fortinet to FireEye, numerous Former Fortinet Employees accessed the Salesforce Database at higher-than-normal frequencies in order to steal Fortinet Trade Secrets related to Fortinet sales, leads, customers (current and future), distributors, pricing, and other confidential sales information. As their departure dates neared, Former Fortinet Employees who would login to the Salesforce Database only occasionally during the normal course of their employment (*e.g.*, once or twice a month) began secretly logging into the database with urgency. In fact, two Former Fortinet Employees logged into the Salesforce Database on their last day at Fortinet and one Former Fortinet Employee illegally logged in two days *after* leaving Fortinet.

35. On information and belief, the Former Fortinet Employees accessed the Salesforce Database during their final days at Fortinet with the intent to steal and did steal Fortinet Trade Secrets for, or on behalf of, FireEye and for the benefit of FireEye.

36. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by Former Fortinet Employees with access to the Salesforce Database by improper means. On information and belief, FireEye has used and disclosed those Fortinet Trade Secrets without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of themselves and others. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

37. FireEye also knowingly and intentionally induced, or attempted to induce, the Former Fortinet Employees to violate their contractual obligations to Fortinet by stealing Fortinet Trade Secrets from the Salesforce Database.

38. By and through their theft of Fortinet Trade Secrets from Fortinet's Salesforce Database, FireEye and the Former Fortinet Employees deliberately intended to disrupt and did disrupt the business relationships between Fortinet and its customers and distributors. FireEye and the Former Fortinet Employees were aware of Fortinet's relationships and/or potential relationships with the customers and distributors listed in the Salesforce Database, yet willfully and intentionally interfered with those potential economic advantages to Fortinet's detriment by unlawfully stealing information about them to use against Fortinet in sales competitions. On information and belief, FireEye has in fact relied upon confidential information, including Fortinet Trade Secrets, stored in the Salesforce Database in furthering FireEye's business interests.

**COUNT I**  
**INFRINGEMENT OF U.S. PATENT NO. 8,056,135**

39. Fortinet incorporates by reference Paragraphs 1 through 38 as if set forth here in full.

40. Fortinet owns all right, title, and interest in and to the '135 patent, titled "Systems and Methods for Updating Content Detection Devices and Systems." The USPTO duly and legally issued the '135 patent on November 8, 2011. A true and correct copy of the '135 patent is attached to this First Amended Complaint as Exhibit A.

41. By virtue of its ownership of the '135 patent, Fortinet maintains all rights to enforce the '135 patent.

42. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '135 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

43. FireEye indirectly infringes the '135 patent by knowingly and intentionally inducing the infringement of the '135 patent by its customers and end users of the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '135 patent. On information and belief, FireEye has

intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the Complaint, FireEye has had knowledge of the '135 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '135 patent.

44. FireEye also contributes to the infringement of the '135 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, FireEye's products, including those identified above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

45. On information and belief, FireEye's infringement of the '135 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

46. As a direct and proximate result of FireEye's infringement of the '135 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

47. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '135 patent, Fortinet will be greatly and irreparably harmed.

48. On information and belief, FireEye's infringement of the '135 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT II**  
**INFRINGEMENT OF U.S. PATENT NO. 8,204,933**

49. Fortinet incorporates by reference Paragraphs 1 through 48 as if set forth here in full.

50. Fortinet owns all right, title, and interest in and to the '933 patent, titled "Systems and Methods for Content Type Classification." The USPTO duly and legally issued the '933 patent on June 19, 2012. A true and correct copy of the '933 patent is attached to this First Amended Complaint as Exhibit B.

51. By virtue of its ownership of the '933 patent, Fortinet maintains all rights to enforce the '933 patent.

52. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '933 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the

FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

53. FireEye indirectly infringes the '933 patent by knowingly and intentionally inducing the infringement of the '933 patent by its customers and end users of the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '933 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of the Complaint, FireEye has had knowledge of the '933 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '933 patent.

54. FireEye also contributes to the infringement of the '933 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, FireEye's products, including those identified



above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

55. On information and belief, FireEye's infringement of the '933 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

56. As a direct and proximate result of FireEye's infringement of the '933 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

57. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '933 patent, Fortinet will be greatly and irreparably harmed.

58. On information and belief, FireEye's infringement of the '933 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT III**  
**INFRINGEMENT OF U.S. PATENT NO. 7,580,974**

59. Fortinet incorporates by reference Paragraphs 1 through 58 as if set forth here in full.

60. Fortinet owns all right, title, and interest in and to the '974 patent, titled "Systems and Methods for Content Type Classification." The USPTO duly and legally issued the '974 patent on August 25, 2009. A true and correct copy of the '974 patent is attached to this First Amended Complaint as Exhibit C.

61. By virtue of its ownership of the '974 patent, Fortinet maintains all rights to enforce the '974 patent.

62. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '974 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

63. FireEye indirectly infringes the '974 patent by knowingly and intentionally inducing the infringement of the '974 patent by its customers and end users of the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Protection System(s) and Virtual Execution (VX) Engine are integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '974 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of this First Amended

Complaint, FireEye has had knowledge of the '974 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '974 patent.

64. FireEye also contributes to the infringement of the '974 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, FireEye's products, including those identified above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

65. On information and belief, FireEye's infringement of the '974 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

66. As a direct and proximate result of FireEye's infringement of the '974 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

67. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '974 patent, Fortinet will be greatly and irreparably harmed.

68. On information and belief, FireEye's infringement of the '974 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT IV**  
**INFRINGEMENT OF U.S. PATENT NO. 7,979,543**

69. Fortinet incorporates by reference Paragraphs 1 through 68 as if set forth here in full.

70. Fortinet owns all right, title, and interest in and to the ‘543 patent, titled “Systems and Methods for Categorizing Network Traffic Content.” The USPTO duly and legally issued the ‘543 patent on July 12, 2011. A true and correct copy of the ‘543 patent is attached to this First Amended Complaint as Exhibit D.

71. By virtue of its ownership of the ‘543 patent, Fortinet maintains all rights to enforce the ‘543 patent.

72. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the ‘543 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated.

73. FireEye indirectly infringes the ‘543 patent by knowingly and intentionally inducing the infringement of the ‘543 patent by its customers and end users of the

FireEye Malware Analysis System and Virtual Execution (VX) Engine including supported FireEye products into which the FireEye Malware Analysis System and Virtual Execution (VX) Engine are integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '543 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of this First Amended Complaint, FireEye has had knowledge of the '543 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '543 patent.

74. FireEye also contributes to the infringement of the '543 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, FireEye's products, including those identified above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

75. On information and belief, FireEye's infringement of the '543 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

76. As a direct and proximate result of FireEye's infringement of the '543 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

77. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '543 patent, Fortinet will be greatly and irreparably harmed.

78. On information and belief, FireEye's infringement of the '543 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT V**  
**INFRINGEMENT OF U.S. PATENT NO. 8,051,483**

79. Fortinet incorporates by reference Paragraphs 1 through 78 as if set forth here in full.

80. Fortinet owns all right, title, and interest in and to the '483 patent, titled "Systems and Methods for Updating Content Detection Devices and Systems." The USPTO duly and legally issued the '483 patent on November 1, 2011. A true and correct copy of the '483 patent is attached to this First Amended Complaint as Exhibit E.

81. By virtue of its ownership of the '483 patent, Fortinet maintains all rights to enforce the '483 patent.

82. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '483 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported

FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

83. FireEye indirectly infringes the '483 patent by knowingly and intentionally inducing the infringement of the '483 patent by its customers and end users of the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '483 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of this First Amended Complaint, FireEye has had knowledge of the '483 patent and by continuing the actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '483 patent.

84. FireEye also contributes to the infringement of the '483 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing



manner. Additionally, on information and belief, FireEye's products, including those identified above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

85. On information and belief, FireEye's infringement of the '483 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

86. As a direct and proximate result of FireEye's infringement of the '483 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

87. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '483 patent, Fortinet will be greatly and irreparably harmed.

88. On information and belief, FireEye's infringement of the '483 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT VI**  
**INFRINGEMENT OF U.S. PATENT NO. 8,276,205**

89. Fortinet incorporates by reference Paragraphs 1 through 88 as if set forth here in full.

90. Fortinet owns all right, title, and interest in and to the '205 patent, titled "Systems and Methods for Updating Content Detection Devices and Systems." The USPTO duly and legally issued the '205 patent on September 25, 2012. A true and correct copy of the '205 patent is attached to this First Amended Complaint as Exhibit F.

91. By virtue of its ownership of the '205 patent, Fortinet maintains all rights to enforce the '205 patent.

92. On information and belief, FireEye has directly infringed, actively induced the infringement of, and/or contributorily infringed one or more claims of the '205 patent, including but not limited to Claim 1, in violation of 35 U.S.C. § 271 by (a) making, using, selling, offering for sale, and/or importing into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated; and/or (b) actively inducing others to make, use, sell, offer for sale, and/or import into the United States and this District products and services including but not limited to the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated.

93. FireEye indirectly infringes the '205 patent by knowingly and intentionally inducing the infringement of the '205 patent by its customers and end users of the FireEye Malware Protection Cloud including supported FireEye products into which the FireEye Malware Protection Cloud is integrated or otherwise incorporated. On information and belief, FireEye's current Vice President of Product Management—Fortinet's former Vice President, Product Management and Product Marketing—has intimate knowledge of Fortinet's patent portfolio including but not limited to the '205 patent. On information and belief, FireEye has intentionally hired other employees from Fortinet; those employees also have awareness of Fortinet's patent portfolio given the prominent discussion(s) of Fortinet's patents and intellectual property rights with its employees. And, at a minimum, since at least the filing of this First Amended Complaint, FireEye has had knowledge of the '205 patent and by continuing the

actions described above has had the specific intent to or was willfully blind to the fact that its actions would induce infringement of the '205 patent.

94. FireEye also contributes to the infringement of the '205 patent because FireEye knows that its products are made for use in infringement and are not staple articles of commerce suitable for substantial non-infringing uses. FireEye's products, including those enumerated above, which it sells directly to consumers as well as through its distribution partners, are designed to be used (and are used by consumers and end-users) in an infringing manner. Additionally, on information and belief, FireEye's products, including those identified above, were especially designed, made, or adapted for use in an infringing manner. FireEye's products have no substantial non-infringing uses and are material to the claimed inventions.

95. On information and belief, FireEye's infringement of the '205 patent is willful and deliberate, and justifies an increase in damages of up to three times in accordance with 35 U.S.C. § 284.

96. As a direct and proximate result of FireEye's infringement of the '205 patent, Fortinet has suffered monetary damages in an amount not yet determined, and will continue to suffer damages in the future unless FireEye's infringing activities are enjoined by this Court.

97. Unless a permanent injunction is issued enjoining FireEye and its officers, agents, employees, and persons acting in active concert or participation with them from infringing the '205 patent, Fortinet will be greatly and irreparably harmed.

98. On information and belief, FireEye's infringement of the '205 patent is exceptional and entitles Fortinet to attorneys' fees and costs under 35 U.S.C. § 285.

**COUNT VII**  
**MISAPPROPRIATION OF TRADE SECRETS**  
**(Cal. Civ. Code § 3426 *et seq.*; Del. Code tit. 6, § 2001 *et seq.*)**

99. Fortinet incorporates by reference Paragraphs 1 through 98 as if set forth here in full.

100. “Fortinet Trade Secrets” as used herein means (i) customer and potential customer names, contacts, lists, purchasing histories, purchasing preferences, and purchasing forecasts, among other proprietary customer information and intelligence such as the identity of key corporate “decision makers”; (ii) key business partner, distributor, wholesaler, and value-added reseller names, contacts, and lists, including but not limited to key downstream companies in the sales channel; (iii) non-public product, pricing, marketing, and sales information, including sales histories, trends, forecasts, plans, techniques, methods, processes, product characteristics, product tests, and other proprietary competitive knowledge and intelligence; (iv) non-public, unique human resources information and employee-specific information, including but not limited to confidential Fortinet competitive salary and compensation package information; and (v) other information owned by Fortinet that was stolen by FireEye, former Fortinet employees, and other persons acting for, on behalf of, or at the direction of FireEye that are legally protected as trade secrets.

101. Prior to FireEye’s thefts, the Fortinet Trade Secrets gave Fortinet a significant competitive advantage over its existing and would-be competitors, including FireEye. This advantage, at least as to FireEye, was compromised as a result of FireEye’s unlawful activities.

102. Fortinet invested substantial resources to develop the Fortinet Trade Secrets. And the Fortinet Trade Secrets derive independent economic value, actual or potential,

from not being generally known to the public or to other persons who can obtain economic value from their disclosure or use.

103. Fortinet made reasonable efforts under the circumstances to maintain the confidentiality of the Fortinet Trade Secrets. Fortinet's efforts included, but are not limited to, (i) having employees and consultants who may have access the Fortinet Trade Secrets sign confidentiality agreements that oblige them not to disclose the Fortinet Trade Secrets or characteristics of the Fortinet Trade Secrets; (ii) limiting the circulation of said materials within Fortinet; (iii) protecting, limiting, and controlling access to Fortinet properties with security cards, and other physical or electronic means; (iv) protecting, limiting, and controlling access to computers with secure log-in identifications and passwords; (v) limiting each employee's access to electronic files to those that the particular employee needs to access (*i.e.*, information segregation); (vi) educating employees on the nature of Fortinet's information that is confidential and proprietary; and (vii) reminding employees on a regular and periodic basis of their obligation to protect and maintain Fortinet's confidential and proprietary information.

104. Fortinet did not consent to the use of any of the Fortinet Trade Secrets by anyone other than authorized Fortinet employees using them for Fortinet's own business purposes.

105. On information and belief, as discussed above, certain former Fortinet employees entered into an agreement with FireEye whereby they would misappropriate Fortinet Trade Secrets in order to give FireEye an unfair advantage in the network security marketplace.

106. On information and belief, at least the Former Fortinet Employees (now FireEye employees) willfully and intentionally misappropriated Fortinet Trade Secrets by acquiring, disclosing, and/or using Fortinet Trade Secrets for FireEye's purposes—for example,

by selling or attempting to sell certain FireEye products, services, or other offerings that would compete with Fortinet's—even though such employees owed a duty to Fortinet to maintain the confidentiality of the Fortinet Trade Secrets.

107. FireEye has illegally obtained Fortinet Trade Secrets as set forth above and through other means of which Fortinet presently is unaware.

108. On information and belief, at all times FireEye knew or had reason to know that Fortinet Trade Secrets were obtained from Fortinet by improper means.

109. On information and belief, FireEye has used and disclosed Fortinet Trade Secrets without Fortinet's consent and without regard to Fortinet's rights, and without compensation, permission, or licenses for the benefit of themselves and others.

110. FireEye's conduct was, is, and remains willful and wanton, and was taken with blatant disregard for Fortinet's valid and enforceable rights.

111. FireEye's wrongful conduct has caused and, unless enjoined by this Court, will continue in the future to cause irreparable injury to Fortinet. Fortinet has no adequate remedy at law for such wrongs and injuries. Fortinet is therefore entitled to a permanent injunction restraining and enjoining FireEye and its agents, servants, officers, directors, and employees, and all persons acting there under, in concert with, or on their behalf, from further using in any manner Fortinet Trade Secrets.

112. In addition, as a proximate result of FireEye's misconduct, Fortinet has suffered actual damages, and FireEye has been unjustly enriched.

113. FireEye's misappropriation of Fortinet Trade Secrets was willful and malicious; on information and belief, FireEye misappropriated Fortinet's trade secrets with the

deliberate intent to injure Fortinet's business and improve its own. Fortinet is therefore entitled to enhanced damages and reasonable attorneys' fees.

**COUNT VIII**  
**INTENTIONAL INTERFERENCE WITH**  
**CONTRACTUAL RELATIONS**

114. Fortinet incorporates by reference Paragraphs 1 through 113 as if set forth here in full.

115. Valid agreements existed between Fortinet and the Former Fortinet Employees whom FireEye induced to steal and/or with whom FireEye was complicit with in stealing Fortinet Trade Secrets and other proprietary and confidential information during and after their Fortinet employment.

116. At all times herein mentioned, FireEye knew that the Former Fortinet Employees had a duty under their employment agreements not to work for or assist any competitor of Fortinet, such as FireEye, and not to disclose confidential or Fortinet Trade Secrets to any competitor of Fortinet including FireEye.

117. Despite such knowledge, FireEye intentionally and without justification solicited, induced, and encouraged the Former Fortinet Employees to breach their contracts with Fortinet.

118. As a direct and proximate result of FireEye's efforts and inducements, the Former Fortinet Employees breached their contracts with Fortinet and prevented performance thereof.

119. As a result of said breaches substantially caused by FireEye, Fortinet has suffered damages and will imminently suffer further damages, including the loss of its competitive position and lost profits, in an amount to be proven at trial.



120. FireEye performed the aforementioned conduct with malice, fraud, and oppression, and in conscious disregard of Fortinet's rights.

121. Accordingly, Fortinet is entitled to recover exemplary damages from FireEye in an amount to be determined at trial.

**COUNT IX**  
**INTENTIONAL INTERFERENCE WITH PROSPECTIVE  
ECONOMIC ADVANTAGE AND/OR RELATIONS**

122. Fortinet incorporates by reference Paragraphs 1 through 121 as if set forth here in full.

123. Through its legitimate business efforts, Fortinet has developed economic relationships with existing and potential customers (such as the above-mentioned Law Firm) and existing and potential business partners (such as the above-mentioned Distributor) that contain the probability of future economic benefits to Fortinet including, but not limited to, the sale of its network security appliances, services, and support platforms.

124. On information and belief, FireEye utilized valuable Fortinet confidential and proprietary information without authorization to illegally and improperly compete with Fortinet for sales of network security appliances, services, and support.

125. On information and belief, FireEye has intentionally and purposefully offered for sale and/or sold to Fortinet's existing and probable customers network security appliances, services, and support based on proprietary information that FireEye illegally and improperly stole from Fortinet including customer names, contacts, and information related to key corporate "decision makers."

126. On information and belief, FireEye has intentionally and purposefully solicited business relationships with Fortinet business partners (such as the above-mentioned

Distributor) based on proprietary information that FireEye illegally and improperly stole from Fortinet.

127. On information and belief, FireEye knew or should have known of Fortinet's past and probable business relationships with its existing and potential customers when it offered for sale and/or sold network security appliances, services, and support based on information that it illegally and improperly obtained from Fortinet.

128. On information and belief, FireEye knew or should have known of Fortinet's past and probable business relationships with existing and potential business partners when it solicited its own business relationships with such third parties.

129. Through at least FireEye's above improper acts, FireEye has knowingly and intentionally acted to disrupt Fortinet's existing and probable business relationships and has disrupted one or more of such relationships.

130. As a direct and proximate result of FireEye's intentional and improper interference with Fortinet's prospective business advantage, as described above, Fortinet has been damaged and continues to suffer damages.

#### **DEMAND FOR JURY TRIAL**

131. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Fortinet demands a jury trial on all triable issues.

#### **REQUEST FOR RELIEF**

WHEREFORE, Fortinet respectfully prays for:

a. A judgment that FireEye has infringed and continues to infringe one or more claims of each of the Asserted Patents;

b. A judgment that FireEye's infringement of the Asserted Patents is willful and deliberate, and therefore that Fortinet is entitled to treble damages under 35 U.S.C. § 284;

c. A permanent injunction enjoining FireEye, its directors, officers, agents, and employees, and those acting in privity or in concert with them, and their partners, subsidiaries, divisions, successors, and assigns, from further acts of infringement, contributory infringement, or inducement of infringement of the Asserted Patents;

d. An award of damages adequate to compensate Fortinet for FireEye's infringement of the Asserted Patents, including all pre-judgment and post-judgment interest, costs, and that the damages so adjudged be increased by the Court pursuant to 35 U.S.C. § 284;

e. A judgment that this is an exceptional case and that Fortinet be awarded attorneys' fees, costs, and expenses incurred in this action;

f. A judgment that Fortinet be awarded damages as a result of FireEye's misappropriation of Fortinet's trade secrets;

g. A judgment that FireEye be ordered to pay exemplary damages due to its willful and malicious misappropriation of Fortinet's trade secrets with deliberate intent to injure Fortinet's business and improve its own;

h. A judgment that Fortinet be awarded damages as a result of FireEye's intentional interference with Fortinet's contracts;

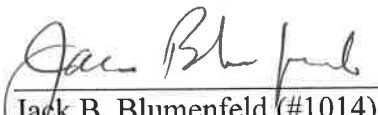
i. A judgment that Fortinet be awarded damages as a result of FireEye's intentional interference with Fortinet's prospective business and economic advantage and/or relations;

j. A permanent injunction enjoining FireEye, its agents, officers, assigns and others acting in concert with it from further wrong-doing, and to return all Fortinet Trade Secrets and other confidential and proprietary materials;

k. A judgment that Fortinet be awarded pre-judgment and post-judgment interest on any award; and

l. That the Court award Fortinet any other relief as the Court deems just and proper.

MORRIS, NICHOLS, ARSHT & TUNNELL LLP



---

Jack B. Blumenfeld (#1014)  
Michael J. Flynn (#5333)  
1201 North Market Street  
P.O. Box 1347  
Wilmington, DE 19899  
(302) 658-9200  
jblumenfeld@mnat.com  
mflynn@mnat.com

OF COUNSEL:

John M. Neukom  
Charles K. Verhoeven  
Andrew M. Holmes  
QUINN EMANUEL URQUHART  
& SULLIVAN LLP  
50 California Street, 22nd Floor  
San Francisco, CA 94111  
(415) 875-6600

*Attorneys for Plaintiff*

September 28, 2012

**CERTIFICATE OF SERVICE**

I hereby certify that on September 28, 2012, I caused the foregoing to be electronically filed with the Clerk of the Court using CM/ECF, which will send notification of such filing to all registered participants.

I further certify that I caused copies of the foregoing document to be served on September 28, 2012, upon the following in the manner indicated:

FireEye, Inc.  
c/o Incorporating Services, Ltd.  
3500 South DuPont Highway  
Dover, DE 19901

*VIA HAND DELIVERY*

  
\_\_\_\_\_  
Jack B. Blumenfeld (#1014)